☑001/003

67,108-043
Wong 1

# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| Applicant: | Wong, Marcus |
| Serial No.: | 09/827,226 |
| Filed: | April 5, 2001 |
| Group Art Unit: | 2136 |
| Examiner: | Shiferaw, Eleni, A. |
| Title: | SYSTEM AND METHOD FOR PROVIDING SECURE COMMUNICATIONS BETWEEN WIRELESS UNITS USING A COMMON KEY |

## REPLY BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appellant now submits this reply brief in response to the Examiner's Answer mailed on May 11, 2007.

The Hwang '99 reference unquestionably states twice that the common secret session key CK is a random number. "We let ... CK be a common secret session key of length 255b of the secure teleconference chosen randomly." (Hwang '99, p. 1470, col. 1, lines 15, 18-19) The network center NC "chooses nonzero random numbers CK and $r_0$, CK being a common secret session key of the secure conference." (p. 1471, col. 1, lines 8-9).

The Examiner's interpretation of CK as a function of the session key-decryption key $r_i$ is directly contrary to those express teachings. Therefore, the Examiner's interpretation is unreasonable and there is no *prima facie* case of anticipation.

1

It appears that the Examiner is interpreting the inclusion of the random number CK into an encryption strategy as a basis for contending that the random number CK is not actually a random number (despite Hwang's express statements that it is) but is actually a function of the session key-decryption key $r_i$. In "Steps 7-9" of column 1 on page 1471, the Hwang '99 reference describes an encryption strategy where the network center (NC) takes the random number CK and then computes public information PI based on the random number CK. Then the NC determines several values (Q, y and R) based on the value of PI. The NC then broadcasts Q, y, R and another value (PA) to the teleconference participants $T_i$. A receiving participant then uses its decryption key $r_i$ to decrypt the broadcast information so that the participant determines the value of the random number CK, which was chosen randomly and encrypted by the NC. The way that a participant in the teleconference arrives at CK does include using "mod $r_i$" as part of the decryption of the broadcast information but that does not somehow change the random number CK into a function of the decryption key $r_i$. Once CK is randomly selected by the NC, it remains unchanged by the encryption and decryption of steps 7-9 so that it is still a random number when it is determined by the participants of the teleconference.

The Examiner's interpretation of steps 7-9 of the Hwang '99 reference as rendering CK a function of the decryption key $r_i$ is unreasonable. The decryption key $r_i$ allows a participant to determine what the random number CK is through decryption but does not render CK a function of $r_i$. Nothing about steps 7-9 changes the random number CK from a random number into a function of another number (the decryption key $r_i$ or any other number for that matter).

2

☑003/003

67,108-043
Wong 1

There is no anticipation and the rejection under 35 U.S.C. §102(b) based upon the Hwang '99 reference must be reversed.

Respectfully submitted,
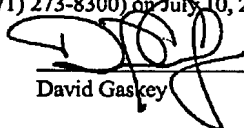
CARLSON, GASKEY & OLDS, P.C.

_____July 10, 2007_____
Date

David J. Gaskey
Registration No. 37,139
400 W. Maple, Suite 350
Birmingham, MI 48009
(248) 988-8360

---

**CERTIFICATE OF FACSIMILE**

I hereby certify that this Reply Brief, relative to Application Serial No. 09/827,226 is being facsimile transmitted to the Patent and Trademark Office (Fax No. (571) 273-8300) on July 10, 2007.

_____
David Gaskey

---

3